Session 306

Authorization API

Craig Keithley
Security and Cryptography Technology Manager
Worldwide Developer Relations

Session 306

Authorization API

Michael Brouwer
Technical Lead Data Security Group

Introduction

- Discuss the recommended usage of the Authorization API
- Make Mac OS X more secure and configurable by adopting this API

What You'll Learn

- Learn to build Applications that need privileged system access
- Learn to build installers that can install privileged application components
- Learn ways to access privileged system calls without running your entire application with root privileges

What This Session Will Cover

- Understanding Authorization
- What it does and doesn't do
- Authorization API

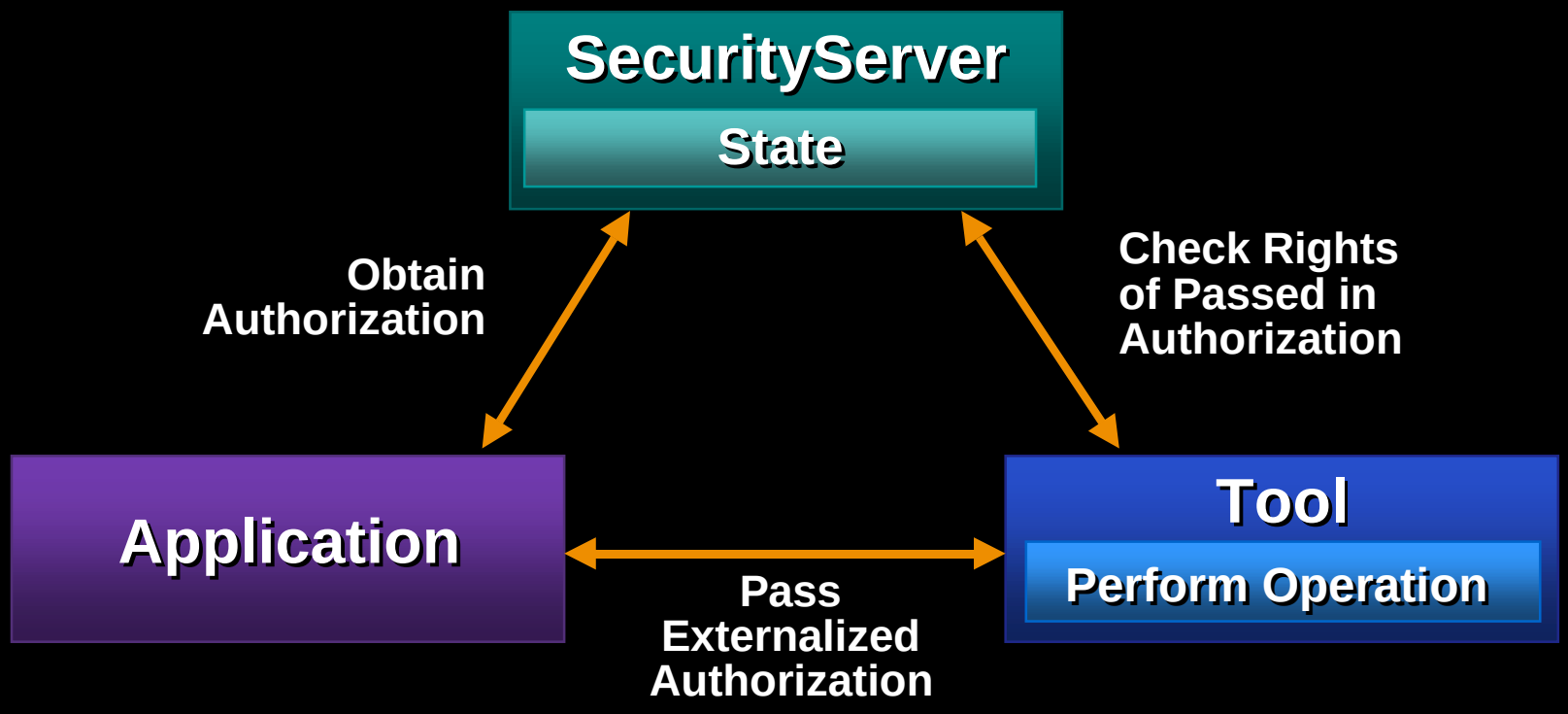
Understanding Authorization

- Understanding Authorization vs. Authentication
- Why use Authorization
  - Better than conventional ad-hoc methods for performing Authorization
  - Make an explicit decision and allow for fine grain control of who can do what

Benefits of Centralized Authorization

- Easier to audit
- Configurable/securable
- Flexible
- Explicit vs. ad hoc

Recommended Architecture



What It Does and Doesn't Do

- Password based only
- Using netinfo
- Answers the "do I have the right to do this" question, but doesn't grant access
- Mac OS X is not a capability based operating system
- Provides user interaction when necessary

Authorization API

- Naming of rights
- Application communication
- Recommended usage of Authorization API
- Temporary solution for 3rd-party installers

Naming of Rights

- Rights are in a hierarchical namespace
- We define domain, but not individual rights since each application has different needs
- Example right names:
  - system.login.console
  - system.login.remote
  - system.admin.reboot
  - system.admin.shutdown
  - system.privilege.admin
  - system.volume.removable.mount

Application Communication

- Split off security sensitive operations into small well understood tools
- Passing Authorization tokens between processes

Authorization and Pre-authorization

- Apps may pre-authorize for the rights needed
- The tool performing the operation should call CopyRights again without the preauthorize flag
- Keep the final call to CopyRights as close as possible to the operation
- Allows addition of audit logging
- Allows for zero length timeouts or removable tokens

Recommended Usage of Authorization API (App)

- Create an AuthorizationRef
- Use CopyRights to figure out what is currently allowed
- When the user wishes to make changes perform a pre-authorization using CopyRights and ask for the rights you need
- Pass the AuthorizationRef to a privileged tool/daemon by Externalizing the AuthorizationRef

Recommended Usage of Authorization API (Tool)

- Call CreateFromExternal to obtain the AuthorizationRef passed in by the application
- Use CopyRights to determine whether the right needed has been granted
- Perform the requested operation(s) (if permitted by CopyRights)

Recommended Architecture

Temporary Solution for Third-Party Installers

- AuthorizationExecuteWithPrivileges
- Right required:
  - System.privilege.admin

Summary

- “Rights” are not capabilities
- Your Application should not run with root privileges
- Preauthorize “rights” and pass them to the tool
- Keep the privileged tool as small as possible and audit it

Resources

Security
Specifications and SDKs
http://developer.apple.com/macos/security.html

CDSA 2.0
Specifications
http://www.opengroup.org

PC/SC
Specifications
http://www.pcscworkgroup.com

Related Sessions

305 Security: Overview An overview of security on Mac OS X	Room A1 **Wed., 9:00am**
307 Security: Keychain High-level access to the keychain	Room J2 **Wed., 2:00 pm**
309 Security: Kerberos Learn about Kerberos	Room A2 **Thus., 2:00 pm**
FF113 Feedback Forum: Security Talk to us	Room C **Fri., 10:30 a.m.**

Who to Contact

Craig Keithley
Apple Worldwide Developer Relations,
Security and Cryptography Technology Manager
keithley@apple.com

Q&A

Craig Keithley
Security and Cryptography Technology Manager
keithley@apple.com

http://developer.apple.com/events/urls.html

WWDC

Worldwide Developers Conference 2001